

A Guerra Cibernética entre a Palestina e Israel

Coronel Patrick D. Allen, Reserva do Exército dos EUA e
Tenente-Coronel Chris Demchak, Exército dos EUA

A guerra cibernética é a guerra da próxima fronteira — um combate conduzido em uma dimensão eletrônica etérea de zeros e números um. O Coronel Patrick D. Allen e o Tenente-Coronel Chris C. Demchak estabelecem uma crônica das recentes escaramuças cibernéticas e discutem as medidas que os EUA podem tomar para serem vitoriosos no espaço cibernético.

O assalto atual dos ataques cibernéticos contra os websites israelenses importantes é talvez o mais extensivo, coordenado e malicioso esforço dos hackers da história.

—Peggy Weigle, Diretora-Executiva da Sanctum Inc.¹

Isto é apenas uma pequena amostra do que está por vir.

—James Adams, Diretor-Executivo de iDefense.²

EM SETEMBRO DE 2000, *hackers* adolescentes israelenses criaram um *website* para interferir nos *websites* do Hezbollah e do Hamas no Líbano. Os adolescentes iniciaram um constante ataque bloqueando o serviço e interferindo em seis *websites* pertencentes às organizações anteriormente mencionadas no Líbano e à Autoridade Nacional Palestina. Este ataque, aparentemente de pouca importância, deu início a uma guerra cibernética que rapidamente escalou para o nível de um incidente internacional. Os palestinos e outras organizações islâmicas clamaram por uma Guerra Santa Cibernética, também conhecida por *ciber-Jihad* ou *e-Jihad*.³ Logo depois, os *hackers* atacaram três conhecidas *webpages* israelenses pertencentes ao Parlamento (o *Knesset*), o Ministério do Exterior e à Força de Defesa de Israel.⁴ Mais tarde, os *hackers* atacaram o Gabinete do Primeiro Ministro israelense, o Banco de Israel e a Bolsa de Valores de Tel Aviv.⁵

Embora os efeitos a longo prazo da guerra cibernética Palestina-Israelense sejam relativamente irrelevantes e nunca causaram uma séria ameaça física a qualquer das nações envolvidas, os elementos do conflito são significativos uma vez que servem como modelo para futuros conflitos cibernéticos.

As escaramuças cibernéticas entre os EUA e a China, em maio de 2001, teve aspectos similares ao incidente entre os palestinos e israelenses. Hoje em dia quase esquecemos que esse incidente por pouco não afetou severamente a distribuição de eletricidade no estado da

Califórnia.⁶ Se tivessem sido bem-sucedidos, o prejuízo que teria causado aos residentes da Califórnia e ao prestígio e segurança dos EUA é difícil de estimar. Os *hackers* chineses penetraram com sucesso numa rede de testes de uma companhia de eletricidade na Califórnia.⁷ As lições resultantes destes conflitos cibernéticos devem ser aprendidas para podermos apropriadamente compreender e estar preparados para o inevitável componente cibernético dos conflitos futuros.

Em setembro de 2000, hackers adolescentes israelenses criaram um website para interferir nos websites do Hezbollah e do Hamas no Líbano. Os adolescentes iniciaram um constante ataque bloqueando o serviço e interferindo em seis websites pertencentes às organizações anteriormente mencionadas no Líbano e à Autoridade Nacional Palestina. Este ataque, aparentemente de pouca importância, deu início a uma guerra cibernética que rapidamente escalou para o nível de um incidente internacional.

O Ciclo do Conflito Cibernético

O conflito entre os *hackers* palestinos-israelenses começou em 1999, mas aumentou dramaticamente logo após os problemas sociais de 28 de setembro de 2000. Em fins de janeiro de 2001, o conflito havia afetado mais de 160 sites israelenses e cerca de 35 palestinos, incluindo, pelo menos, um site americano. A partir de julho de 1999, até meados de abril de 2002, dos 1.295 sites desconfigurados na região do Oriente Médio, 548 foram *websites* israelenses (.il) e outros tantos sofreram obstruções

severas em seus serviços.⁸ Os dois tipos principais de ataques consistiram em desconfiguração dos websites e bloqueio da distribuição do serviço (*distributed denial of service — DDoS*). A desconfiguração dos *websites* tende a se concentrar nos sites políticos de grande relevância, tais como os pertencentes ao governo. Em alguns casos as transações comerciais foram afetadas durante dias devido as desconfigurações constantes de *websites*.⁹ Os servidores dos websites usados pelos *hackers* de um lado para iniciar os ataques foram empregados, com frequência, pelos *hackers* do lado oposto para iniciar ataques parecidos.¹⁰ Os códigos empregados por um lado eram re-escritos pelo lado oposto, que por sua vez

Um hacker simpatizante dos palestinos conhecido por Dodi desconfigurou um provedor da Internet que fornecia serviços aos cidadãos israelenses idosos, deixando uma mensagem afirmando categoricamente que ele podia fechar a ISP Net Vision israelense, que serve de nó para quase 70% do tráfico da Internet em Israel. . . . A Internet Clandestina Israelense (Israeli Internet Underground — IIU), formada por um grupo de hackers que se uniram para ajudar na segurança dos websites israelenses, afirma que já há evidência de ataques da quarta fase. Isso inclui a destruição de websites comerciais com capacidades de comércio eletrônico que, segundo o IIU, causou uma queda de oito por cento na bolsa de valores israelense.

iniciava um contra-ataque.¹¹ Os ataques empregando o método *DDoS* fecharam os sites do lado oposto por vários dias e acrescentaram mais estresse à infra-estrutura da Internet da região.¹²

Além disso, ataques foram iniciados contra companhias provedoras de infra-estrutura de telecomunicações, tais como a *AT&T*, que aparentemente foi contratada para ajudar a incrementar a largura de banda dos sites israelenses, alvos dos *hackers*.¹³ Um *hacker* simpatizante dos palestinos conhecido por Dodi desconfigurou um provedor da Internet que fornecia serviços aos cidadãos israelenses idosos, deixando uma mensagem afirmando categoricamente que ele podia fechar a ISP Net Vision israelense, que serve de nó para quase 70% do tráfico da Internet em Israel.¹⁴

Aproximadamente em 8 de novembro de 2001, o *Unity*, um grupo extremista mulçumano com laços com o Hez-bollah, anunciou que havia iniciado a terceira fase de uma

estratégia consistente de 4 fases. A primeira fase visava afetar seriamente os websites do governo israelense. A segunda previa ataques ao Banco de Israel e à bolsa de valores de Tel Aviv. A terceira compreendia objetivos tais como a infra-estrutura do *ISP* israelense e o servidor da *Lucent and Golden Lines*, um provedor israelense de telecomunicações. A *Unity* divulgou que não executaria a quarta fase, isto é, a fase final, especificamente a destruição de sites de comércio eletrônico, ameaçando assim a perda de milhões de dólares em transações.¹⁵

A Internet Clandestina Israelense (*Israeli Internet Underground — IIU*), formada por um grupo de *hackers* que se uniram para ajudar na segurança dos websites israelenses, afirma que já há evidência de ataques da quarta fase. Isso inclui a destruição de websites comerciais com capacidades de comércio eletrônico que, segundo o *IIU*, causou uma queda de oito por cento na bolsa de valores israelense.¹⁶

Apesar da pirataria cibernética ter existido entre *hackers* americanos e chineses nos últimos anos, o choque da aeronave de reconhecimento americana *EP-3* com o interceptor chinês *F-8* foi o incidente que iniciou o conflito principal. Os *hackers* chineses aumentaram suas atividades contra os EUA e tentaram organizar um esforço de pirataria cibernética de grande escala durante a primeira semana de maio de 2001.¹⁷

Agindo da mesma forma que os palestinos, os chineses criaram um website no qual *hackers* voluntários poderiam obter instrumentos e técnicas necessários para começar um programa denominado *USA Kill*.¹⁸ O Centro de Proteção de Infra-Estrutura Nacional dos EUA fez um alerta, em 26 de abril de 2001, para todos os websites do governo e comerciais.¹⁹ Enquanto isso, *hackers* americanos, motivados pela detenção prolongada da tripulação do *ER-3* na China, começaram a organizar o programa *China Killer*.²⁰ Quando os *hackers* chineses declararam uma trégua, afirmaram que haviam desconfigurado ou bloqueado o serviço de mais de 1000 websites americanos. Os *hackers* americanos, aparentemente, causaram o mesmo nível de danos nos websites chineses.

Quatro Fases de Futuros Conflitos Cibernéticos

Os conflitos cibernéticos :

- Envolvem um período inicial de surpresa, seguido por um período mais prolongado de adaptação e recuperação.
- Intensificam-se rapidamente e ampliam seus efeitos à medida que os atacantes procuram encontrar objetivos vulneráveis.
- Desenvolvem-se rapidamente em conflitos internacionais à medida que *hackers* voluntários tomam uma posição a favor ou contra as distintas facções.
- Aumentam o ritmo de desenvolvimento de armas cibernéticas e da subsequente proliferação.

- Baseado em observações dos conflitos entre a Palestina e Israel e entre China e Estados Unidos, acreditamos que o futuro conflito cibernético desenvolver-se-á em quatro fases.

Fase 1: Surpresa e adaptação. A guerra cibernética palestina-israelense é um exemplo de como uma nação pode ser surpreendida por um ataque cibernético. Os *hackers* adolescentes israelenses inicialmente surpreenderam os websites que apoiavam a causa palestina com seus ataques empregando o método *DDoS*. Quando os palestinos declararam um *ciber-Jihad* contra Israel os *hackers* pró-Palestina alcançaram um nível comparável de surpresa contra os sites israelenses que

havia sido selecionados como alvos. Os israelenses ficaram surpresos ao saber que seus próprios cidadãos tinham iniciado o conflito cibernético. Também se surpreenderam pela magnitude da resposta pró-Palestina e pela vulnerabilidade dos sites governamentais e comerciais. Depois do choque inicial, cada lado passou por um período de reparação dos danos causados aos sistemas e de melhoramento das defesas contra ataques futuros.

Vale a pena considerar os efeitos iniciais do conflito. *Jerusalembooks.com*, o provedor de livros eletrônicos mais importante de Israel, teve que parar suas atividades durante dias devido a um ataque de desconfiguração da rede. A companhia enfrentou vários dias de perdas em vendas e o risco de uma prolongada desconfiança por parte de seus clientes referente à segurança das transações feitas pela rede.²¹ Da mesma maneira, o *website* do Gabinete de Administração de Terras de Israel teve que permanecer fechado durante meses.²² Para Israel, em geral, tais fechamentos criaram uma falta de confiança. Além disso, a grande quantidade de ataques *DDoS* (mais de 115 na região entre 6 de outubro e 2 de dezembro de 2000) causou um grande estresse na já delicada infra-estrutura da Internet do Oriente Médio.²³ O custo de um ataque cibernético é geralmente maior para os alvos comerciais do que para os sites governamentais. Como disse Lawrence Gershwin, assessor de tecnologia de maior hierarquia da CIA em um testemunho prestado perante o Congresso: “Nossa sociedade ligada por fios coloca a todos nós — em particular os negócios americanos porque devem manter um intercâmbio aberto com os clientes — num nível de risco elevadíssimo com relação aos inimigos.”²⁴



Quando um site governamental fica fora do ar ou é desconfigurado, a nação talvez seja um pouco humilhada. Não entanto, quando o site de uma companhia sai do ar, ela perde lucro. Matt Krantz e Edward Iwata afirmaram o seguinte num artigo publicado pelo jornal *USA Today* “Alguns negócios perdem de US\$10.000,00 até vários milhões de dólares por minuto quando seus sites saem fora do ar... Perdem, em média de US\$100.000,00 por hora em produtividade”.²⁵ A companhia de pesquisa *Reality Research* avaliou que os negócios em todo o mundo podem ter perdido mais de US\$1.5 trilhão de dólares no ano passado como consequên-

cia dos assaltos cibernéticos.²⁶

Apesar de os sites comerciais terem interesse em se defender contra ataques cibernéticos, o desejo de ser mais custo eficiente faz com que a maioria das companhias ignore as vulnerabilidades da rede até que seja vítima de um ataque pelos *hackers*.²⁷ Portanto, existe uma neces-

Vale a pena considerar os efeitos iniciais do conflito. Jerusalembooks.com, o provedor de livros eletrônicos mais importante de Israel, teve que parar suas atividades durante dias devido a um ataque de desconfiguração da rede. A companhia enfrentou vários dias de perdas em vendas e o risco de uma prolongada desconfiança por parte de seus clientes referente à segurança das transações feitas pela rede.

sidade de criar incentivos maiores para que os negócios obtenham maior segurança no espaço cibernético, e deveriam existir penalidades para aqueles que não estiverem seguros em uma determinada data.

Fase 2: Rápida ampliação horizontal. O conflito cibernético palestino-israelense se ampliou rapidamente. Nas primeiras quatro semanas do conflito, *hackers* pró-palestinos atacaram um site americano. Três semanas mais tarde, *hackers* israelenses atacaram sites no Irã e no Líbano.²⁸ Comparado com os palestinos, Israel contava com mais sites desde os quais podia iniciar contra-ataques.

Portanto os *hackers* israelenses começaram a procurar websites vulneráveis fora da Autoridade Nacional Palestina e do Líbano. Por exemplo, um grupo de *hackers* israelenses, que se chamavam de *Mossad*, desconfigurou o website do presidente iraniano, afirmando que o Irã apoiava as organizações terroristas no Líbano.

A guerra cibernética se ampliou horizontal e mais rapidamente que a guerra padrão por três motivos. Em primeiro lugar, o principal critério para escolher alvos para ataques por parte dos *hackers* civis é a vulnerabilidade e não a importância. A busca de alvos vulneráveis é intensificada até que se encontre um. Se os sites governamentais ou comerciais na nação objetivo não são

Quanto mais bipolar um conflito, como o árabe-israelense, maior é a possibilidade de atrair elementos que desejam trabalhar por um dos lados. Cada lado percebe o outro como tendo aliados permanentes que sempre respaldarão seus inimigos.

Em conseqüência, os EUA foram declarados um alvo juntamente com Israel, pouco tempo após o começo do conflito cibernético palestino-israelense.

... O grau de participação internacional que se observa nos conflitos cibernéticos tem paralelos impressionantes com o grau de participação de voluntários observados durante a Guerra Civil espanhola, uma precursora da II GM.

suficientemente vulneráveis, os sites das nações amigas da nação a que pretende atacar se convertem em alvos. Por outro lado, *hackers* profissionais, empregados por uma nação específica, provavelmente só intensificarão seus ataques o necessário para obter os efeitos desejados na nação alvo.

Em segundo lugar, grupos internacionais de *hackers* vêem a situação como uma na qual podem exercer o poder sem temer um contra-ataque. Muitos *hackers* querem demonstrar que apóiam uma causa. Uma vez que a *Web* contém métodos de difusão pública próprios, *hacking* (violar sistemas de computação) qualquer alvo que pertença à *Web* tende a ganhar notoriedade.

Em terceiro lugar, os conflitos cibernéticos, até agora, têm sido polarizados, ou bipolares. Quanto mais bipolar um conflito, como o árabe-israelense, maior é a possibilidade de atrair elementos que desejam trabalhar por um dos lados. Cada lado percebe o outro como tendo aliados permanentes que sempre respaldarão seus inimigos. Em conseqüência, os EUA foram declarados um alvo juntamente com Israel, pouco tempo após o começo

do conflito cibernético palestino-israelense.²⁹

Tradicionalmente, os aliados dos países em guerra estavam numa situação bastante segura no que diz respeito a possíveis ataques militares, a menos que participassem diretamente no combate. O custo para envolver uma nação neutra no combate, em geral, incorria em pelo menos alguma penalidade à nação que estava optando por escalar o conflito. No espaço cibernético, no entanto, o custo de tal escalada é pequeno para uma nação e quase inexistente para um *hacker* individual. Portanto, a escalada horizontal ocorrerá provavelmente em futuros conflitos cibernéticos.

Fase 3: Rápida internacionalização de entidades não-estatais. O conflito cibernético tende a atrair dois tipos de atores. O primeiro tipo inclui grupos de *hackers* talentosos que se encontram, com frequência, envolvidos em incidentes cibernéticos internacionais. O segundo consiste de *hackers* amadores atraídos por um fervor patriótico ou ideológico. O conflito cibernético palestino-israelense atraiu *hackers* provenientes de Israel, Palestina, Líbano, Alemanha, Arábia Saudita, Paquistão, Brasil e Estados Unidos. A maioria dos ataques contra Israel foram iniciados de fora desse país ou da Autoridade Nacional Palestina.³⁰ Vale a pena ressaltar que um ou mais grupos brasileiros de *hackers* atacaram ambos os lados do conflito palestino-israelense, aparentemente para demonstrar quem eram os participantes de cada lado. A escaramuça cibernética chinesa-americana atraiu *hackers* simpatizantes dos EUA, Arábia Saudita, Paquistão, Índia, Brasil, Argentina e Malásia. Dentro do grupo de *hackers* simpatizantes do lado chinês se encontravam alguns provenientes da China, Japão, Indonésia e Coréia. Deve-se mencionar que a ideologia política dos *hackers* não era necessariamente a mesma da nação, exceto naquelas onde o governo controla rigidamente o uso da Internet.

O grau de participação internacional que se observa nos conflitos cibernéticos tem paralelos impressionantes com o grau de participação de voluntários observados durante a Guerra Civil espanhola, uma precursora da II GM. O conflito entre facistas de um lado e comunistas e democratas do outro, atraiu um grande número de voluntários estrangeiros a ambos os lados. Tanto na Guerra Civil espanhola como no conflito cibernético palestino-israelense, a ideologia, e não o lucro, foi o que motivou aqueles voluntários. Existem *hackers* mercenários, mas não há confirmação de que estiveram em atividade no conflito palestino-israelense ou no chinês-americano.

A maioria dos *hackers* envolvidos nos conflitos mencionados anteriormente eram veteranos de anteriores guerras cibernéticas internacionais. Os *hackers* paquistaneses, por exemplo, tinham também estado envolvidos na desconfiguração de *Webpages* na Índia e certos *hackers* brasileiros haviam participado na descon-

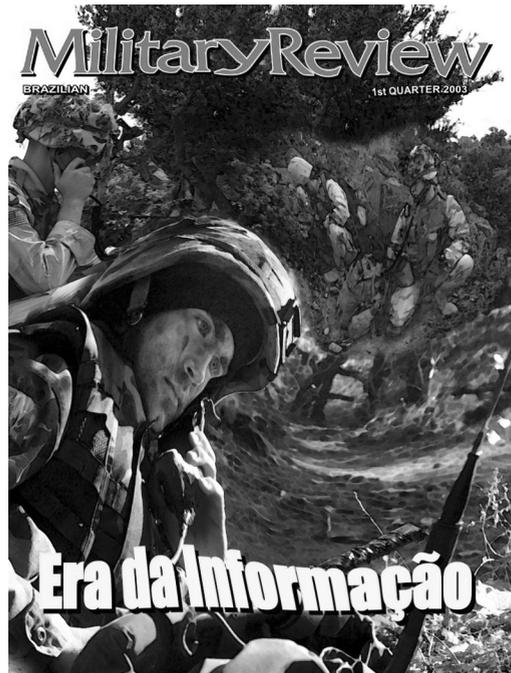
figuração de *Webpages* americanas.³¹ *Hactivism* ou seja a atividade de atacar os sites é tentador quando os *hackers* têm o poder de participar do cenário internacional.³²

Um *hacker*, ou um grupo pequeno de *hackers*, pode causar um enorme dano em pouco tempo. Durante o conflito chinês-americano, um grupo de *hackers* denominado *PoizonB0x* afetou, com muito êxito, mais de 400 sites chineses (*.cn).³³ Um estudo estimou que somente havia uns 30 *hackers* principais envolvidos no conflito cibernético palestino-israelense que proporcionavam os instrumentos, enquanto outros envolvidos na digitação, proporcionavam a força bruta, checando e certificando-se das vulnerabilidades dos alvos em potencial.³⁴ Essa força bruta, pesquisando a série de endereços 209 IP permitiu aos *hackers* chineses descobrirem a presença de uma rede de teste de transmissão de energia elétrica desprotegida no estado da Califórnia.³⁵

Mesmo que o ataque inicial cibernético de um futuro conflito seja uma ação militar bem coordenada, voluntários provenientes de várias nações provavelmente estarão envolvidos em ataques similares, complicando assim as operações de combate da guerra real. Esta ameaça por si só tem numerosas implicações para a soberania nacional e o direito internacional.

Fase 4: Aprendizagem global e o aumento do desenvolvimento e proliferação de armas cibernéticas. Os instrumentos empregados e aperfeiçoados para executar a pirataria cibernética no conflito palestino-israelense logo apareceram em outras ações internacionais e nacionais de pirataria cibernética. Durante a guerra cibernética palestina-israelense, os *hackers* israelenses desenvolveram um novo instrumento para o método de ataque *DDoS*. Nos EUA, *hackers* adolescentes adquiriram o referido instrumento dos *hackers* israelenses e planejaram um ataque global à Internet, que seria executado no primeiro dia do ano 2001. Se o FBI não tivesse sido alertado sobre a conspiração, o ataque poderia ter impossibilitado o uso da Internet naquele dia.³⁶

Durante a escaramuça cibernética entre os Estados Unidos e a China foi lançado o ataque *Carko DDoS*.³⁷ O agente do mencionado ataque não apenas tentou derrubar o sistema alvo. Também lançou um ataque contra a memória



intermediária (*buffer overflow*), para entrar uma nova senha de *root* ou instalar uma nova porta traseira no sistema alvo, enquanto o mesmo se recuperava do ataque inicial. Isso significava que aqueles sistemas que foram afetados pelos ataques *Carko* deveriam ser examinados para detectar a existência de *software* que poderia permitir entradas posteriores no sistema.

Embora os ataques *DDoS* fossem conhecidos e empregados antes deste conflito, a capacidade de uma pessoa, com largura de banda limitada, executar um ataque *DDoS* de grande escala é um acontecimento recente.

O *hacker* pode empregar um modem de 56 Kb e uma linha de assinatura digital assimétrica (*ADSL*) para começar um ataque, que posteriormente será aumentado 10.000 vezes, por difusores de serviços da rede, para gerar ataques de uma magnitude de dois terços de uma linha *T1*. “Com ferramentas como estas, um modem de 56 Kb pode converter-se em uma arma poderosa e sua largura de banda é irrelevante”

Um hacker, ou um grupo pequeno de hackers, pode causar um enorme dano em pouco tempo. Durante o conflito chinês-americano, um grupo de hackers denominado PoizonB0x afetou, com muito êxito, mais de 400 sites chineses (.cn). Um estudo estimou que somente havia uns 30 hackers principais envolvidos no conflito cibernético palestino-israelense que proporcionavam os instrumentos, enquanto outros envolvidos na digitação, proporcionavam a força bruta, checando e certificando-se das vulnerabilidades dos alvos em potencial.*

ressalta Ben Venzke da *iDefense*.³⁸ Portanto, um pequeno número de ataques coordenados empregando laptops através de modems pode gerar um ataque combinado equivalente a várias linhas *T1* ou até mesmo uma *T3*. Tal ataque poderia devastar a maioria dos sistemas.

Além dos ataques *DDoS* lançados desde sites de difusão, existe uma técnica através da qual os *hackers* podem colocar software em outros websites da Internet e posteriormente

ativá-lo em um determinado momento. Estes websites infectados são denominados zumbis já que participam, inconscientemente, em ataques DDoS. O FBI descobriu que 560 websites em 220 sites da Internet haviam sido infectados para um único e amplo ataque DDoS.³⁹

Em geral, o índice de desenvolvimento de armas cibernéticas tende a aumentar durante os conflitos cibernéticos, assim como a invenção de novas armas é mais rápida e comum durante a guerra. Entretanto, o que é mais desafiador é que o ritmo de proliferação de armas cibernéticas é muito mais rápido do que o das armas tradicionais.

Implicações para a Política

Baseado nestes acontecimentos existem quatro necessidades na política nacional e internacional:

- Decidir quem irá proporcionar segurança na Web.
- Oferecer respostas legais à rápida escalada horizontal.
- Atribuir responsabilidade legal para os cidadãos *hackers* responsáveis por incidentes internacionais.
- Deter a proliferação de armas cibernéticas.

Durante a escaramuça cibernética entre os Estados Unidos e a China foi lançado o ataque Carko DDoS. O agente do mencionado ataque não apenas tentou derrubar o sistema alvo. Também lançou um ataque contra a memória intermediária (buffer overflow), para entrar uma nova senha de root ou instalar uma nova porta traseira no sistema alvo, enquanto o mesmo se recuperava do ataque inicial.

Quem proporcionará segurança na Web? A pergunta principal referente à política associada ao custo de executar atos comerciais na Web é: Quem é responsável pela segurança na Web? Os grandes provedores de serviço da Internet, as Corporações, o Governo? Ou permanecerá a Internet sendo uma zona de fogo livre?⁴⁰ Alguns países escolheram atribuir a segurança da Web ao governo, especialmente em países onde a Internet é considerada uma ameaça ao poder absoluto do governo, como na China. A maioria dos países europeus estão promulgando leis que estabelecem o governo como o garante central da segurança da Web. À medida que as economias e as comunicações dependem mais da Internet, os países escolherão opções que os colocarão em algum lugar ao longo do espectro de segurança versus o de privacidade. Na maioria dos casos as leis colocarão a segurança da Web acima da privacidade individual.¹⁴ Os Estados Unidos deverão decidir onde, neste espectro, irão operar e que nível de segurança cibernética deverão proporcionar para

apoiar a segurança das transações e uma certa medida de privacidade.

Resposta legal à rápida escalada horizontal. Quanto mais elevada é a visibilidade do conflito cibernético, mais atrairá *hackers* internacionais, e mais rapidamente os *hackers* buscarão os sites vulneráveis. Quais são as alternativas legais para um país atacado durante um conflito no qual não está envolvido? Para se obter uma resposta legal, a identidade do atacante deve ser estabelecida. Não obstante, com frequência, os ataques cibernéticos não são iniciados por um país, mas por um cidadão. É difícil justificar um bombardeio de retaliação contra *hackers* que violam a neutralidade ou lealdade de sua própria nação para com as outras. A atividade dos *hackers* é uma ameaça assimétrica apresentada por atores não estatais, o que torna difícil justificar um contra-ataque.

Pouco pode ser feito no espaço cibernético contra os *hackers*, já que não se constituem em um objetivo definido. *Hackers* ou grupos de *hackers*, em geral, não possuem uma infra-estrutura que possa servir de alvo, mesmo no espaço cibernético. Quando existe tal infra-estrutura, ter acesso legal à mesma é difícil devido à soberania nacional. Quando os Estados Unidos, por exemplo, realizaram uma operação policial contra dois *hackers* russos, surgiram problemas relacionados com o procedimento adotado, porque o FBI fez uma busca, a longa distância, nos computadores dos respectivos *hackers*.⁴² Qualquer resposta deve considerar o possível dano colateral que pode ser causado por tal retaliação. Uma vez que os *hackers* tendem a conduzir seus ataques através de websites de terceiros, qualquer contra-ataque cibernético deve levar em consideração o fato de que o mesmo pode afetar os servidores de vítimas inocentes.

Acima de tudo, os países precisam definir sua autoridade legal para exercer a soberania, processar e impor penalidades aos *hackers* condenados por ataques cibernéticos. Acordos internacionais para a não proteção de seqüestradores aéreos contribuíram significativamente à redução destes crimes. Acordos internacionais similares com relação ao crime cibernético ajudariam a reduzir os refúgios disponíveis para os *hackers*.

Responsabilidade legal. Cada país deve aceitar o fato de que seus cidadãos *hackers* podem causar incidentes internacionais contrários aos seus interesses. Israel foi arrastado para um conflito cibernético por ações de seus próprios *hackers* adolescentes e não por uma decisão governamental. Israel não estava preparado para travar uma guerra cibernética e era mais vulnerável que seu adversário.

As violações cibernéticas das redes interconectadas on line encontram-se numa área cinzenta das leis de segurança internacionais e nacionais. Para localizar e processar os *hackers*, os países devem depender das autoridades e das leis da nação que abriga o hacker. Israel estimou que os danos causados pelo vírus global denominado *Love*, inclu-

indo a interrupção de serviços de companhias telefônicas celulares, custou uns US\$12 milhões. No entanto, Israel não pôde processar o hacker responsável porque seu país (as Filipinas) só definiu que criar vírus era um delito criminal depois desse acontecimento.⁴³

A penalização criminal é muito difícil quando os *hackers* operam desde um país obviamente hostil. Não obstante, os países têm certos direitos, sob um princípio protetor internacionalmente reconhecido, quando as nações que ofendem não colaboram. Existe um caso de direito internacional, embora limitado, que pode apoiar a ação de um estado como resposta aos ataques cibernéticos. Sob este princípio, quando uma pessoa de um país “A” causa danos aos país “B” e quando o país “A” não faz nada para impedir que este indivíduo continue a causar danos, então o país “B” tem o direito de iniciar uma ação contra o país “A”.⁴⁴ Apesar de este princípio não ter sido ainda aplicado em casos relacionados com a guerra cibernética, o precedente legal existe.

Se um país tem a intenção de tratar os *hackers* como criminosos e terroristas, sua política deverá ser elaborada para extinguir quaisquer atividades dos hackers, mesmo as de menor importância. Tal política de segurança alienaria os seus cidadãos *hackers*. Julgando pelas leis cibernéticas propostas, a maioria das nações européias parece dirigir-se para este caminho.

Provavelmente os EUA não aplicariam esta medida de força sobre seus *hackers* nacionais. Tal medida não apenas seria desnecessária, como também contraproducente. Uma opção que talvez tenha êxito é proporcionar incentivos para os *hackers* de “chapéu branco”. O interesse desses indivíduos é ajudar os outros e não causar prejuízos, portanto deveriam ser incentivados para que localizassem as vulnerabilidades e ajudassem os administradores de sistemas a aplicar os devidos *patches*. Agentes de segurança governamentais ou particulares poderiam verificar se o *patch* é correto e se não inclui uma porta de acesso traseira. Os *hackers* de “chapéu branco” poderiam ser publicamente recompensados e contratados como assessores independentes para outras aplicações. O trabalho desses *hackers* deveria ser recompensado, porém, não deveriam necessariamente ser controlados ou empregados oficialmente pelo governo. A imagem de independência, além do fato de fazer o que é correto,



é um grande atrativo para os *hackers* de chapéu branco.

Por outro lado, os *hackers* de “chapéu preto” devem ser identificados e processados. O sistema legal precisa desenvolver uma completa gama de sanções formais contra a pirataria cibernética e suas diversas atividades. Hoje, as agências estatais e federais nos EUA estão totalmente desqualificadas para lidar com o grau e o nível das ações dos *hackers*.⁴⁶ O governo tem grande dificuldade para atrair e manter peritos em computação, devido ao baixo salário que oferece.⁴⁷

Uma alternativa talvez fosse empregar os *hackers* de “chapéu branco” para detectar os de “chapéu preto” no espaço cibernético. Forças militares de

elite dedicadas a evitar, desviar, avariar, rastrear e castigar ataques contra os interesses cibernéticos globais e dos EUA, talvez possam manter a ordem na Web e evitar a intensificação dos conflitos cibernéticos.⁴⁸

Resposta Internacional

Cada escaramuça cibernética incentiva o desenvolvimento de novas armas cibernéticas, que são rapidamente disseminadas para os *hackers* profissionais e amadores em todo o mundo. A proliferação tem conseqüências significativas na monitoração das ferramentas de *hacking* empregadas nos conflitos e em novas tecnologias da Internet em geral. Além de monitorar a capacidade dessas novas ferramentas, as nações precisam monitorar as “salas de bate-papo” usada pelos *hackers* amadores que não podem resistir a tentação de brincar com o novo brinquedo. (Os *hackers* patrocinados por um estado não empregarão a nova arma a menos que seja parte de um plano geral, para que não percam o elemento de surpresa). Portanto, cada país deve desenvolver contramedidas para auxiliar na prevenção do emprego de novas armas cibernéticas ou reduzir seus efeitos. Os servidores devem ser escaneados regularmente para detectar a existência de *software* zumbi, que permite a execução de ataques *DDoS*, minimizando assim a magnitude de futuros ataques. Mantendo-se atualizada sobre as novas ferramentas e métodos de *hacking*, uma nação estará melhor preparada para prever e minimizar seus efeitos.

Em qualquer conflito moderno, o espaço cibernético pode ser uma via de acesso adicional. Sendo o mais importante no

ambiente político internacional, os EUA passaram a ser um pára-raios para *hackers* e ataques terroristas, que não levam em consideração se a nação está ou não envolvida no conflito inicial. Até 11 de setembro de 2001, os EUA eram, em geral, complacentes com seus

inimigos de além mar. No entanto, a distância entre os EUA e seus inimigos foi drasticamente reduzida. As lições dos primeiros conflitos cibernéticos devem ser aprendidas agora para estar melhor preparado para os conflitos futuros. **MR**

Referências

1. Peggy Weigle, executiva da Sanctum Inc., citada em Carmen J. Gentile, "Hacker War Rages In Holy Land", disponível na Internet no endereço www.wired.com/news/politics/0,1283,40030,00.html, 8 de novembro de 2000.
2. James Adam, executivo, iDefense, citado em Gentile, "Israeli Hackers Vow to Defend", na Internet www.wired.com/news/politics/0,1283,40187,00.html, 15 de novembro de 2000.
3. "Cyber War also Rages in MidEast", The Associated Press, na Internet no endereço www.wired.com/news/print/0,1294,39766,00.html, 26 de outubro de 2000; Brian Krebs, "Hackers Worldwide Fan Flames in Middle East Conflict", disponível no endereço www.infowar.com/hacker/00/hack_112000c_j.shtml, 20 de novembro de 2000.
4. "Cyber War Also Rages in MidEast".
5. Krebs, "Hackers Worldwide"; Infowar.com, 20 de novembro de 2000; "Israel's Mossad Hackers Break into Iranian President's Website", Xinhua News Agency Bulletin (18 de janeiro de 2001); disponível no endereço www.infowar.com/hacker/01/hack_011901c_j.shtml, 19 de janeiro de 2001; Tania Hershman, "Israeli Seminar on Cyberwar", disponível no endereço www.wired.com/news/politics/0,1283,41048,00.html, 10 janeiro de 2001.
6. Gentile, "Palestinian Crackers Share Bugs", disponível no endereço www.wired.com/news/politics/0,1283,40449,00.html, 2 de dezembro de 2000.
7. Robyn Welsman, "California Power Grid Hack Underscores Threat to U.S.", disponível no endereço www.newsfactor.com/perl/story/11220.html, 13 de junho de 2001.
8. "Israel Suffers Escalating Hack Attacks", disponível no endereço www.mi2g.com/cgi/mi2g/press/150402.php, 15 abril 2002.
9. Gentile, "Israeli Hackers."
10. *Ibid.*, "Palestinian Crackers."
11. *Ibid.*, "Hacker War Wages."
12. *Ibid.*, "Israeli Hackers."
13. Krebs; Elisa Batista, "Palestinian Group Targets AT&T", disponível no endereço www.wired.com/news/business/0,1367,39913,00.html, 6 de novembro de 2000.
14. Gentile, "Israeli Hackers."
15. *Ibid.*, "Hacker War Wages."
16. *Ibid.*, "Israeli Hackers."
17. Michelle Delio, "It's (Cyber) War: China vs. U.S.", disponível no endereço www.wirednews.com/news/print/0,1294,43437,00.html, 30 de abril de 2001.
18. *Ibid.*
19. Aviso Nº. 01-009 do Centro de Proteção da Infra-Estrutura Nacional dos EUA., "Increased Internet Attacks Against U.S. Web Sites and Mail Servers Possible in Early May", disponível no endereço www.nipc.gov/warnings/advisories/2001/01-009.htm, 26 de abril de 2001.
20. Delio, "U.S., Chinese Hackers Wage Online War", Agence France Presse (24 de abril de 2001), disponível no endereço www.inq7.net/int/2001/apr/24/inf_3-1.htm, 24 de abril de 2001.
21. Gentile, "Palestinian Crackers" e "Israeli Hackers."
22. Elazar Levin, "Overseas Hackers Strike Again: Israel Land Administration Shuts Down Most of its Web Site", Israel's Business Arena (4 de dezembro de 2000), disponível no endereço <http://new.globes.co.il/serveEN/globes/docView.asp?did=454769&fid=947>, e www.infowar.com/hacker/00/hack_120500a_j.shtml, 5 de dezembro de 2000.
23. Gentile, "Palestinian Crackers."
24. Lawrence K. Gershwin, "Cyber Threat Trends and US Network Security", numa declaração perante o Comitê Econômico Conjunto, disponível no endereço www.cia.gov/cia/public_affairs/speeches/gershwin_speech_062, 21 de junho de 2001.
25. Matt Krantz e Edward Iwata, "Companies Bleed Cash When Computers Quit", USA Today, 11 de junho de 2001, seção B, p. 1.
26. "Israel Suffers."
27. Delio, "Got a Virus? Blame the Tightwads", disponível no endereço www.wired.com/news/technology/0,1282,42047,00.html, 28 de fevereiro de 2001.
28. "Cyber War Also Rages"; Krebs, "Hackers Worldwide."
29. Gentile, "Hacker War Rages."
30. *Ibid.*, "Israeli Hackers."
31. Robert MacMillan, "Hackers Deface Policy.com as 'Public Service'", Newsbytes, Washington, D.C., disponível no endereço www.infowar.com/hacker/00/hack_111500a_j.shtml, 15 de novembro de 2000.
32. Carrie Kirby, "Hacking with a Conscience is a New Trend", San Francisco Chronicle, 20 de novembro de 2000, disponível no endereço www.infowar.com/hacker/00/hack_112400a_j.shtml, 24 de novembro de 2000.
33. John Lyman, "Hackers Aim at Computer Security Sites", disponível no endereço www.newsfactor.com/perl/printer/11230, 14 de junho de 2001.
34. Gentile, "Palestinian Crackers."
35. Welsman, "California Power Grid."
36. Krebs, "FBI Arrests Hacker in Planned New Year's Eve Attack", Newsbytes, Washington, D.C. (12 de janeiro de 2001), disponível no endereço www.infowar.com/hacker/01/hack_011501b_j.shtml, 15 de janeiro de 2001; e "Feds Warn of Concerted Hacker Attacks on New Year's Eve", Newsbytes, Washington, D.C., disponível no endereço www.infowar.com/hacker/00/hack_122900a_j.shtml, 29 de dezembro de 2000.
37. Steve Gold, "More Details Emerge on Expected Chinese Hack Attacks", Newsbytes, Parsippany, Nueva Jersey (27 de abril de 2001), disponível no endereço www.infowar.com, 27 de abril de 2001.
38. Gentile, "Palestinian Crackers."
39. Krebs, "Feds Warn...".
40. Chris C. Demchak, "State Security Paths in a Digital Mass Society: New Internet Topologies and Security Institution Obligations", Cambridge Review of International Affairs, número especial sobre a segurança do estado e na internet, com data desconhecida.
41. Bob Sullivan, "Cybercrime Treaty Targets Hackers", MSNBC News, disponível no endereço www.msnbc.com:80/news/480734.asp, 6 de novembro de 2000, e www.infowar.com/hacker/00/hack_110600e_j.shtml, 6 de novembro de 2000.
42. Thomas C. Greene, "FBI Hacked Russian Hackers", disponível no endereço www.theregister.co.uk/content/8/18496.html, 25 de abril de 2001.
43. Israeli Consulate Online Service (IsraelLine), "Love Virus Hits Israeli Businesses", Nova York, 8 de maio de 2000; Lynn Burke, "Love Bug Case Dead in Manila", Wired Online, 21 de agosto de 2001.
44. Iain Cameron, Protective Principle of International Criminal Jurisdiction (Dartmouth, Massachusetts: Dartmouth Publishing Company, 1993).
45. Sullivan, "Cybercrime Treaty."
46. Greg Farrell, "Police Outgunned by Cybercriminals", USA Today, 6 de dezembro de 2000, disponível no endereço www.infowar.com, 7 de dezembro de 2000.
47. Patrick Thibodeau, "CIO Panel Recommends Hiring IT Rookies", Computerworld, disponível no endereço <http://iwsun4.infoworld.com/articles/hn/sml/00/10/12/001012hnhiring.xml>, 12 de outubro de 2000.
48. Demchak, "State Security Paths."

O Coronel Patrick D. Allen pertencente ao Componente da Reserva do Exército dos EUA. É o engenheiro de sistemas de maior hierarquia no Sistema de Informação Avançada da General Dynamics, Operações de Informação, em Arlington, Virgínia. Obteve os títulos de Bacharel em Física e de Mestre em Engenharia Industrial e Pesquisa de Operações; obteve um segundo mestrado em Estudos Estratégicos e é PhD em Economia Mineral e Pesquisa Operacional. Além disso é graduado da Escola de Comando e Estado-Maior do Exército dos EUA, da Escola Superior de Guerra do Exército y da Escola Superior de Guerra da Força Aérea. Tem mais de 40 artigos publicados referentes aos temas de programação, simulação e operações de informação.

A Tenente-Coronel Chris C. Demchak, do Componente da Reserva do Exército dos EUA, é co-fundadora do Grupo de Pesquisa de Política do Espaço Cibernético, um grupo transnacional de peritos que documentam e estudam a expansão global das tecnologias da Web e seus efeitos em agências nacionais militares e outras. Ela obteve os títulos de Mestre em Desenvolvimento Econômico e em Engenharia de Energia, e é PhD em Ciências Políticas com especialização em Teoria da Organização e Sistemas Complexos. Esteve encarregada e dirigiu estudos empíricos e profundos sobre os exércitos dos EUA, da Grã-Bretanha e de Israel e da análise das implicações da modernização democrática civil-militar nas FA da Europa Central. Muitos de seus artigos foram publicados, bem como seu livro intitulado Military Organizations, Complex Machines: Modernization in the U.S. Armed Services.